Datenschutzerklärung gemäß EU-DSGVO

für die Durchführung der elektronischen Führerscheinkontrolle

Fleet-Hub verify

Fleet-Hub GmbH
Dr.-Gustav-Adolph-Str. 2 I 82049 Pullach
Handelsregisternummer: HRB 252221 | Registergericht: Amtsgericht München
Geschäftsführer: Sascha Bopp, Marcus Federhoff
info@fleethub.de

Revision: 03. Februar 2024

I. Inhaltsverzeichnis

1. Einleitung

Diese Datenschutzerklärung liefert Betroffenen im Sinne der EU-DSGVO eine transparente Aufklärung zum Umgang mit personenbezogenen Daten im Hinblick auf die Anwendung *Fleet-Hub verify*. *Fleet-Hub verify* ist ein Produkt der *Fleet-Hub GmbH,* im Folgenden kurz *Fleet-Hub* genannt, einem gemäß deutschem Recht eingetragenen Unternehmen mit Sitz in der Dr.-Gustav-Adolph-Str. 2 in 82049 Pullach.

2. Rechtsgrundlage für die Datenverarbeitung

Im Rahmen der Halterhaftung hat ein Fahrzeughalter wiederkehrend festzustellen, dass ein Fahrer dem ein Fahrzeug überlassen wird, tatsächlich im Besitz einer Fahrerlaubnis ist. Dies gilt insbesondere für die Überlassung von Dienstwagen an Mitarbeiter eines Unternehmens. *Fleet-Hub* verarbeitet personenbezogene Daten zwecks Durchführung der elektronischeren Führerscheinkontrolle mittels *Fleet-Hub verify* Die Rechtmäßigkeit der Verarbeitung ergibt sich aus Art. 6 DSGVO Abs. 1 c. Der zwischen dem Fahrzeughalter/ Arbeitgeber und *Fleet-Hub* geschlossene Dienstleistungs- sowie Auftragsverarbeitungsvertrag zu *Fleet-Hub* stellt die rechtliche Grundlage zur Datenverarbeitung gemäß Art. 13 DSGVO 1 c dar.

3. Standort der Datenverarbeitung

Für den Serverbetrieb hat *Fleet-Hub* die *Hetzner Online GmbH* beauftrag. Das hochmoderne Rechenzentrum mit Zertifizierung gemäß DIN ISO/IEC 27001 befindet sich in Deutschland am Standort Nürnberg. Der Betreiber des Rechenzentrums hat keinen Zugriff auf Ihre personenbezogenen Daten. Die Verarbeitung von personenbezogenen Daten in einem Drittland im Sinne des Art. 13 DSGVO (1) f) findet nicht statt.

4. Umfang der Datenverarbeitung

Als betreffender Nutzer werden folgende personenbezogene Daten von Ihnen erfasst und verschlüsselt gespeichert:

- Vorname
- Nachname
- E-Mail-Adresse
- Handynummer (sofern als Alternative zur E-Mail-Adresse angegeben)
- ID des *Fleet-Hub*-Siegels bei Siegelprüfung
- Führerscheinnummer bei siegelloser Kontrolle
- Zeitstempel und Art der durchgeführten Kontrollvorgänge

Im Zuge einer Kontrolle findet die Erkennung und Echtheitsprüfung eines Führerscheins mittels Web-App statt, indem Bilddaten der Kamera auf dem Smartphone vollautomatisch verarbeitet werden.

5. Datenverwendung

Die beschriebenen Daten werden ausschließlich zum Zweck der elektronischen Führerscheinkontrolle erfasst und gespeichert.

6. Datenweitergabe

Eine Weitergabe der Daten an Dritte findet ausdrücklich nicht statt. Nur der Auftraggeber, also der Halter des Ihnen überlassenen Fahrzeuges, kann auf die verarbeiteten Daten zugreifen.

7. Datenlöschung und -korrektur

Sie haben das Recht die sofortige und vollständige Löschung bzw. Korrektur Ihrer Daten über den Fahrzeughalter bei uns zu beauftragen. Die reguläre Löschfrist für die Historie von Kontrollvorgängen beträgt fünf Jahre.

8. Datenschutzbeauftragter

Als Datenschutzbeauftragter wurde die Project 29 GmbH berufen:

Christian Volkmer (GF),
Projekt 29 GmbH & Co. KG
Ostengasse 14, 93047 Regensburg

datenschutzbeauftragter@datenschutzexperte.de

9. Auskunftsrecht und Datenübertragbarkeit

Sie haben gemäß Art. 15 DSGVO das Recht eine inhaltliche Auskunft über die zu Ihrer Person gespeicherten Daten zu beantragen. Außerdem haben Sie gemäß Art. 20 DSGVO das Recht, die Sie betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, um diese einem anderen Verantwortlichen ohne Behinderung zu übergeben.

10. Beschwerderecht

Jede betroffene Person hat gemäß Art. 77 DSGVO unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstößt.

Technische und organisatorische Maßnahmen

für die Durchführung der elektronischen Führerscheinkontrolle

Fleet-Hub verify

Fleet-Hub GmbH
Dr.-Gustav-Adolph-Str. 2 I 82049 Pullach
Handelsregisternummer: HRB 252221 | Registergericht: Amtsgericht München

Geschäftsführer: Sascha Bopp, Marcus Federhoff
info@fleethub.de

03.02.2024

I. Inhaltsverzeichnis

II. Abkürzungsverzeichnis

DSGVO	Datenschutz-Grundverordnung
HTTP	Hypertext Transfer Protocol
RAID	Redundant Array of Independent Disks
REST	Representational State Transfer
SSH	Secure Shell
TLS	Transport Layer Security
TOM	Technische und organisatorische Maßnahmen

1. Systemstruktur

Die Grobarchitektur des elektronischen Führerscheinkontrollsystems lässt sich als klassische, mobile und verteilte Applikation beschreiben. Dabei kön- nen hinsichtlich der Systemkomponenten der Service-Anbieter einerseits und die Service-Konsumenten andererseits unterschieden werden.

Der Service-Anbieter wird durch unser Rechenzentrum repräsentiert, welches durch eine Firewall vor Angriffen geschützt ist. Sowohl die serviceorientierte Applikationslogik als auch die persistente Datenhaltung werden durch das Rechenzentrum realisiert. Schließlich werden die durch das Rechenzentrum angebotenen Dienste durch Service-Konsumenten in Anspruch genommen.

Als Service-Konsumenten agieren Smartphone- und Web-Applikationen. Die Kommunikation zwischen Serviceanbieter und -Konsumenten findet über *HTTP*-basierte *RESTful* Webservices statt. Zur sicheren Kommunikation authentifizieren sich Service-Konsumenten mittels *Digest Access Authentication* beim Dienstanbieter. Darüber hinaus wird die Datenübertragung mittels *TLS* verschlüsselt. Wartungs- und Entwicklungsaufgaben werden über eine verschlüsselte *SSH*-Verbindung durchgeführt.

Für den Serverbetrieb wurde die *Hetzner Online GmbH* beauftragt. Das hochmoderne Rechenzentrum mit Zertifizierung gemäß DIN ISO/IEC 27001 befindet sich in Deutschland am Standort Nürnberg.

2. Technische und organisatorische Maßnahmen

Die folgenden technischen und organisatorischen Maßnahmen werden für das elektronische Führerscheinkontrollsystem Fleet-Hub verify, in Anlehnung an die DSGVO, verbindlich festgelegt.

2.1 *Vertraulichkeit*

(gemäß Art. 32 Abs. 1 b) DSGVO)

2.1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

2.1.1.1 Rechenzentrum am Standort Nürnberg

- personenbezogene Zutrittsüberwachung
- elektronisches Schließsystem
- Videokameras zur 24/7 Überwachung
- 24/7- Sicherheitsdienst
- Alarmsicherung
- Zutritt nur nach Vier-Augen-Prinzip
- redundante Speicherung der Zutrittsprotokolle
- Hochsicherheitszaun um den gesamten Datacenterpark

2.1.1.2 Client-Arbeitsplätze am Standort Pullach

- elektronisches Schließsystem für Bürogebäude
- protokollierte Schlüsselausgabe
- Alarmsicherung
- 24/7- Sicherheitsdienst

2.1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- persönliche Zugangsdaten bestehend aus Nutzername und sicherem Passwort
- Rechtekonzept mit separatem Administrationsrecht
- Passwortregeln mit Einhaltungszwang *(Mindestlänge von 8 Zeichen, Groß- und Kleinbuchstaben, Ziffern sowie mind. ein Sonderzeichen)*
- automatische Bildschirmsperre nach 5 Minuten Inaktivität an Client-Arbeitsplätzen
- automatische Session-Terminierung nach 24 Minuten Inaktivität für Web-Applikationen
- Firewall mit regelmäßigen Updates
- Festplattenverschlüsselung für Notebooks
- Wartungs- und Entwicklungsaufgaben über verschlüsselte SSH-Verbindungen

2.1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- differenziertes Berechtigungskonzept mit den Rollen Fah*rer*, *Kontrolleur*, *Fuhrparkmanager* und *Administrator*
- persönliche Zugangsdaten bestehend aus Nutzername und sicherem Passwort
- Rechtevergabe nach dem „Need-to-Know“-Prinzip
- Zugriffsprotokoll
- Trennung von Produktiv- und Testsystem

2.1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- vollständige logische Mandantentrennung
- differenziertes Berechtigungskonzept in Abhängigkeit der Funktion im Unternehmen

2.1.5 Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

- Trennung von Produktiv- und Testsystem
- Festplattenverschlüsselung im Rechenzentrum

2.2 *Integrität*

(gemäß Art. 32 Abs. 1 b) DSGVO)

2.2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Über-tragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Daten werden ausschließlich verschlüsselt übertragen
- Zugriffsschutz bei mobilen Endgeräten via PIN

2.2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- protokollierter Datenzugriff
- protokollierte Datenmodifikation

2.3 *Verfügbarkeit und Belastbarkeit*

(gemäß Art. 32 Abs. 1 b) DSGVO)

2.3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

2.3.1.1 Stromversorgung Rechenzentrum

- AC: 230V, 16A
- redundante USV-Anlagen
- Batterie-Betrieb: ca. 15 Minuten
- Netzersatzanlage
- Notstromdiesel für autonomen Betrieb
- Stromversorgung erfolgt über Doppelboden

2.3.1.2 Klimatisierung Rechenzentrum

- energieeffiziente direkte freie Kühlung Redundanz N+2
- Kaltgang-Einhausungen
- Unterboden-Klimaanlage
- überdurchschnittlich hoher Doppelboden
- Temperaturüberwachung der Raumluft
- Temperaturüberwachung in Server-/Verteilerschränken

2.3.1.3 Brandschutz Rechenzentrum

- modernes Brandfrüherkennungssystem mit direkter Verbindung zur örtlichen Feuerwehr
- spezielle Tür- und Schließsysteme

2.3.1.4 Sonstiges

- tägliche automatische Sicherung des kompletten Servers
- verschlüsselte Sicherung in separatem Brandabschnitt
- RAID-System mit permanenter Überwachung
- Hot-Plug zum Austausch von defekten RAID-Festplatten ohne Ausfall
- Monatlicher Test der Backup-Widerherstellung
- zügige Wiederherstellbarkeit des laufenden Betriebes ist möglich gemäß *Art. 32 Abs. 1 c) DSGVO*
- Virenschutz, Spamfilter und Firewall

2.4 *Verfahren zur Überprüfung, Bewertung und Evaluierung*

(gemäß Art. 32 Abs. 1 b); Art. 32 Abs. 1 DSGVO)

2.4.1 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Datenschutzbeauftragter ist bestellt
- Datenschutzschulung von Mitarbeitern
- schriftliche Verpflichtung von Mitarbeitern auf Datengeheimnis
- AV-Vereinbarung mit Hetzner Online GmbH
- Regemäßige Prüfung der TOM-Dokumentation von Hetzner Online GmbH

2.4.2 Datenschutz-Management

Zentrale Verwaltung, Nachvollziehbarkeit und Protokollierung des aktuellen Datenschutzniveaus im Unternehmen.

- interne Datenschutzaudits
- strukturierte Protokollierung von Ergebnissen

2.4.3 Incident-Response-Management

Umfasst den gesamten organisatorischen und technischen Prozess der Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Störungen in IT/Datenschutz-Bereichen berücksichtigen.

- DDoS-Schutz
- Automatische Systemüberwachung mit Reporting im Falle von erkannten Sicherheitsvorfällen
- Meldewege und Prozesse sind bekannt

2.4.4. Datenschutzfreundliche Voreinstellungen

Einstellungen von Soft- und Hardware vor Nutzung und Herausgabe an Benutzer bzw. Kunden.

- Beachtung bei der App-Entwicklung
- Beachtung bei der Konfiguration von Hard- und Softwaresystemen